CLAIMS

We claim:

Claim 1: A method of providing streaming content, comprising the steps of:

creating a digital container that includes contents including streaming media content and digital rights management (DRM);

selecting one or more modules for inclusion in the digital container, the selection of the modules being based on one at least one of a type of streaming media content and the DRM;

encrypting the streaming media content of the digital container to produce a secured streaming container (SSC); and

transmitting the SSC to a target device for access of the SSC from the target device.

Claim 2: The method of claim 1, wherein the transmitting includes transmitting the SSC over at least one of a local area network, a wide-area network, a wireless network, and the Internet.

Claim 3: The method of claim 1, wherein the target device includes one of a cell phone, a personal data assistant (PDA), a personal computer, a computing device, a portable music player, a tablet computer, a cable modem, satellite receiver, a television, and a cable television tuner.

Claim 4: The method of claim 1, wherein the digital container is created by receiving input of at least one of the target device, one or more media files to be included in the digital container, a transaction option type, a digital rights management (DRM) option, a digital container graphic, and a search descriptor data.

Claim 5: The method of claim 4, wherein:

the transaction option type includes a financial transaction type, a transaction update type, a transaction update address, a server address, demographics type, or a subscription type;

the financial transaction type includes at least a credit card type; and

the subscription type includes at least a financial transaction defining a period of time.

Claim 6: The method of claim 4, wherein the creating step includes selecting one or more software modules based on a type of the one or more media files, which control the streaming of the one or more media files in the environment of the target device.

Claim 7: The method of claim 4, wherein the digital container graphic is either a static image and an animated image and is at least one of informational and promotional graphics that appears on a viewable electronic digital container cover before and after the digital container is opened.

Claim 8: The method of claim 1, further comprising encoding the streaming media content for playback by one of a media player resident on the target device and a media player included with the digital container.

Claim 9: The method of claim 1, wherein the streaming media content includes at least one of video, audio, animation, and text content.

Claim 10: The method of claim 1, wherein the streaming media content is one or more streaming media files.

Claim 11: The method of claim 1, further comprising the step of creating one or more secondary files for inclusion in the digital container, the one or more secondary files include at least one of a hypertext markup language (html) file, an image file, and a segment of the one or more media files.

Claim 12: The method of claim 11, wherein the segment is at least one of:

(i) viewable prior to executing a purchase transaction for the media content, and

(ii) unencrypted for previewing.

Claim 13: The method of claim 12, wherein the at least one of an html file and image file are viewable during playing of the one or more streaming files.

Claim 14: The method of claim 1, further comprising the step of providing an execution batch file in the digital container for controlling presentation of the streaming media content in at least one of a preset sequence, a relative sequence, and a timing interval.

Claim 15: The method of claim 14, further comprising the step of establishing limits on access to the streaming media content based on at least one of a period of time and a number of access instances.

Claim 16: The method of claim 15, wherein the establishing limits includes limiting at least one of copying the streaming media content and transferring the streaming media content.

Claim 17: The method of claim 1, further comprising the step of producing informational and search metadata tag sets wherein the tag sets are included in the SSC.

Claim 18: The method of claim 17, wherein the tag sets are unencrypted extensible markup language (XML) tags.

Claim 19: The method of claim 18, wherein the tag sets are used by search engines to discover at least one of the digital container and the streaming media content.

Claim 20: The method of claim 18, wherein the XML tags are manually created.

Claim 21: The method of claim 18, wherein the XML tags describe at least a portion of the streaming media content and provides at least one of a file size and a file type.

Claim 22: The method of claim 18, wherein the XML tags provide access rights data to the target device.

Claim 23: The method of claim 18, wherein the XML tags provide at least one of a content file title, a key word data, and a key phrase data as search descriptors for search engines.

Claim 24: The method of claim 18, wherein the XML tags are substantially compliant with one of Open Mobile Alliance standard (OMA) and Open Data Rights language (ODRL) standard.

Claim 25: The method of claim 1, further comprising the step of registering the SSC with a digital container verification database including one of identifying the SSC and providing date information about the SSC.

Claim 26: The method of claim 25, wherein the registering the SSC occurs automatically when the SSC is created.

Claim 27: The method of claim 1, wherein the transmitting step is via email, file transfer protocol (FTP), download from a web-site, peer-to-peer file sharing, instant messaging, or physical transport.

Claim 28: The method of claim 1, further comprising the step of encoding the digital container for transmission as a hypertext markup (HTML) file.

Claim 29: The method of claim 1, further comprising the step of establishing a transaction type that is to be executed for a user to gain permission to open the SSC, and when executed, the transaction type includes at least one of a password, demographic information, device information, financial data, credit card data, and personal user data.

Claim 30: The method of claim 29, wherein the personal identification includes at least one of a user identification number, a company identification number, and a biometric identification.

Claim 31: The method of claim 30, wherein the biometric information includes at least one of a voice data, a fingerprint data, a retina data, and a physical attribute scan data.

Claim 32: The method of claim 29, wherein the device information includes gathering data from a removable storage media.

Claim 33: The method of claim 29, wherein the transaction type includes a subscription transaction type that, when executed, gathers subscription data enabling a user to purchase multiple digital containers.

Claim 34: The method of claim 33, wherein the subscription transaction type gathers subscription data enabling a user to purchase the multiple digital containers related to a pre-determined time period.

Claim 35: The method of claim 1, wherein the encrypting step includes compressing the contents of the digital container.

Claim 36: The method of claim 1, wherein in the encrypting step a hidden key is incorporated into the digital container.

Claim 37: A method of receiving electronic data, comprising the steps of:

receiving a secured streaming container (SSC) having streaming media content; and

accessing the SSC to acquire portions of the streaming media content while other portions of the streaming media content remain secure in the SSC.

Claim 38: The method of claim 37, further comprising playing the portions of the streaming media content while other portions remain secured in the SSC.

Claim 39: The method of claim 37, wherein the SSC includes digital rights management (DRM) which controls the access to the SSC.

Claim 40: The method of claim 37, wherein the receiving step receives the SSC on a target device.

Claim 41: The method of claim 40, wherein the target device includes at least one of a cell phone, a personal data assistant (PDA), a personal computer, a computing device, a portable music player, a tablet computer, a cable modem, a cable television tuner, and a satellite receiver.

Claim 42: The method of claim 40, wherein at least some of the contents of the SSC is configured to execute within the environment of the target device.

Claim 43: The method of claim 37, further comprising the step of obtaining permission to access the SSC.

Claim 44: The method of claim 43, wherein the obtaining permission includes at least one of (i) verifying a password, (ii) gathering demographic data, (iii) gathering personal data, (iv) gathering of the target device identification data, (v) processing a subscription transaction, and (vi) processing a financial transaction.

Claim 45: The method of claim 44, wherein the personal data includes at least one of a user identification (ID), a company ID, and a biometric data.

Claim 46: The method of claim 44, wherein the target device identification data includes at least one of an input from a removable storage media and an input provided from a secure device attached to a target device.

Claim 47: The method of claim 37, wherein in the accessing step, extensible markup language tags (XML) are read to determine at least one of a content file title, a digital rights management descriptor, a file size and a file type.

Claim 48: The method of claim 37, further including decrypting the SSC.

Claim 49: The method of claim 48, wherein the decrypting includes decompressing the streaming media content.

Claim 50: The method of claim 48, further including decoding the streaming media content as a hyper-text markup language (html) file.

Claim 51: The method of claim 37, further including the step of downloading a java applet in order to read the SSC content.

Claim 52: The method of claim 37, further comprising the step of supplying a password for a subsequent SSC access.

Claim 53: The method of claim 37, further comprising the steps of:

successfully gaining permission to the SSC on a target device;

sending a portion of data which is unique to the target device to a verification server;

combining the portion of data and a digital container identification data previously registered to produce a permission token;

sending the permission token to the target device; and

rekeying an original key sent with the SSC using the permission token to securely rekey the streaming media content so that decrypting the streaming media content is locked to and performed only on the target device.

Claim 54: The method of claim 37, wherein the accessing step further includes:

detecting an attempt to access the SSC;

determining if permission has been previously granted to open the SSC and, if not,

supplying transaction information;

sending the transaction information to a digital container verification server in an encrypted session;

sending a permission token back to the SSC; and

granting permission to open the SSC.

Claim 55: The method of claim 54, wherein transaction information comprises supplying at least one of a financial information, a personal data, and a demographic data.

Claim 56: The method of claim 55, wherein the financial information is credit card information.

Claim 57: The method of claim 55, wherein the personal data is at least one of a biometric data, a personal identification, and a password.

Claim 58: A method of creating and accessing streaming content, comprising the steps of:

creating a digital container that includes contents including at least streaming media content and digital rights management (DRM);

selecting one or more modules for inclusion in the digital container

based on one at least one of a type of streaming media content and the DRM;

encrypting the streaming media content and optionally the DRM to produce a secured streaming container (SSC); and

accessing the secured streaming container (SSC) using the one or more modules to control playback of the streaming media content.

Claim 59: The method of claim 58, further comprising the steps of transmitting the SSC to a target device.

Claim 60: The method of claim 59, wherein the target device includes one of a cell phone, a personal data assistant (PDA), a personal computer, a computing device, a portable music player, a tablet computer, a cable modem, and a cable television tuner.

Claim 61: The method of claim 58, wherein the digital container is created by receiving input of at least one of a target device type, one or more media files to be included in the digital container, transaction option type, digital rights management (DRM) options, digital container graphics, and search descriptor data.

Claim 62: The method of claim 61, wherein:

the transaction option type includes a financial transaction type, a transaction update type, a transaction update address, a server address, demographics type, a subscription type,

the financial transaction type includes at least a credit card type, and

the subscription type includes at least a financial transaction defining a period of time.

Claim 63: The method of claim 58, further comprising the step of selecting one or more modules based on the type of one or more media files and associated with the streaming media content, the one or more modules controlling the streaming of the one or more media files in the environment of the target device type.

Claim 64: The method of claim 58, further comprising encoding the streaming media content which is encoded for playback by one of a media player resident on a target device and a media player included with the digital container.

Claim 65: The method of claim 58, wherein the streaming media content includes at least one of video, audio, animation, and text.

Claim 66: The method of claim 58, further comprising providing an execution batch file in the digital container for controlling the presentation of the streaming media content in at least one of a preset sequence, a relative sequence, and a timing interval.

Claim 67: The method of claim 58, further comprising controlling access to the streaming media content using the DRM on subsequent accesses.

Claim 68: The method of claim 58, further including the steps of:

decrypting the streaming media content; and

playing the streaming media content using a media player.

Claim 69: The method of claim 58, wherein the accessing step further includes:

detecting an access attempt to the SSC;

determining if permission has been previously granted to open the SSC and, if not,

supplying transaction information;

sending the transaction information to a digital container verification server in an encrypted session;

sending a permission token back to the SSC; and

granting permission to open the SSC.

Claim 70: The method of claim 58, further comprising the step of playing the streaming media content such that one or more segments of the streaming media content are sequentially played from the digital container while remaining portions of the streaming media content remain secure in the digital container until sequentially played.

Claim 71: A computer program product comprising a computer usable medium having readable program code embodied in the medium, the computer program product includes at least one component to:

create a digital container that includes contents including streaming media content and digital rights management (DRM);

select one or more modules for inclusion in the digital container wherein the selection of the modules is based on at least one of a type of streaming media content and the DRM;

encrypt the streaming media content of the digital container to produce a secured streaming container (SSC); and

transmit the SSC to a target device for access of the SSC from the target device.

Claim 72: The computer program product of claim 71, wherein the at least one component transmits the SSC over at least one of a local area network, a wide-area network, a wireless network, and the Internet.

Claim 73: The computer program product of claim 71, wherein the at least one component transmits to the device, the device being one of a cell phone, a personal data assistant (PDA), a personal computer, a computing device, a portable music player, a tablet computer, a cable modem, a satellite receiver, a television, and a cable television tuner.

Claim 74: The computer program product of claim 71, wherein the at least one component creates the digital container by receiving input of at least one of a target device type, one or more media files to be included in the digital container, a transaction option type, a digital rights management (DRM) option, a digital container graphic, and a search descriptor data.

Claim 75: The computer program product of claim 74, wherein:

the transaction option type includes a financial transaction type, a transaction update type, a transaction update address, a server address, demographics type, a subscription type,

the financial transaction type includes at least a credit card type, and

the subscription type includes at least a financial transaction defining a period of time.

Claim 76: The computer program product of claim 71, wherein the at least one component selects one or more software modules based on the type of the one or more media files, the one or more software modules adapted to control the streaming of the one or more media files in the environment of the target device type.

Claim 77: The computer program product of claim 74, wherein the digital container graphic is either a static image and an animated image and is at least

one of informational and promotional graphics that appears on a viewable electronic digital container cover before and after the digital container is opened.

Claim 78: The computer program product of claim 71, wherein the at least one component encodes the streaming media content and is encoded for playback by one of a media player resident on the target device and a media player included with the digital container.

Claim 79: The computer program product of claim 71, wherein the streaming media content includes at least one of video, audio, animation, and text content.

Claim 80: The computer program product of claim 71, wherein the streaming media content is one or more streaming media files.

Claim 81: The computer program product of claim 71, wherein the at least one component creates one or more secondary files for inclusion in the SSC, the one or more secondary files include at least one of a hypertext markup language (html) file, an image file, and a segment of the one or more media files.

Claim 82: The computer program product of claim 81, wherein the segment is at least one of:

(i) viewable prior to executing a purchase transaction for the media content, and

(ii) unencrypted for previewing.

Claim 83: The computer program product of claim 81, wherein the at least one of an html file and image file are viewable during playing of the one or more streaming files.

Claim 84: The computer program product of claim 71, wherein the at least one component provides an execution batch file in the digital container for controlling the presentation of the media content in at least one of a preset sequence, a relative sequence, and a timing interval.

Claim 85: The computer program product of claim 84, wherein the at least one component establishes limits on access to the media content based on at least one of a period of time and a number of access instances.

Claim 86: The computer program product of claim 85, wherein the establishing limits includes limiting at least one of copying the media content and transferring the media content.

Claim 87: The computer program product of claim 71, wherein the at least one component produces informational and search metadata tag sets and includes the tag sets in the SSC.

Claim 88: The computer program product of claim 87, wherein the tag sets are unencrypted extensible markup language (XML) tags.

Claim 89: The computer program product of claim 88, wherein the tag sets are used by search engines to discover at least one of the digital container and the streaming media content.

Claim 90: The computer program product of claim 88, wherein the XML tags are manually created.

Claim 91: The computer program product of claim 88, wherein the XML tags describe a least a portion of the streaming media content and provides at least one of a file size and a file type.

Claim 92: The computer program product of claim 88, wherein the XML tags provide access rights data to the device.

Claim 93: The computer program product of claim 88, wherein the XML tags provide at least one of a content file title, a key word data, and a key phrase data as search descriptors for search engines.

Claim 94: The computer program product of claim 93, wherein the XML tags are substantially compliant with one of Open Mobile Alliance standard (OMA) and Open Data Rights language (ODRL) standard.

Claim 95: The computer program product of claim 71, wherein the at least one component registers the SSC with a digital container verification database including at least one of identifying the SSC and providing date information about the SSC.

Claim 96: The computer program product of claim 95, wherein the registering the SSC automatically occurs when the SSC is created.

Claim 97: The computer program product of claim 71, wherein the at least one component transmits using email, file transfer protocol (FTP), download from a web-site, peer-to-peer file sharing, instant messaging, or physical transport.

Claim 98: The computer program product of claim 71, wherein the at least one component encodes the digital container for transmission as a hypertext markup (HTML) file.

Claim 99: The computer program product of claim 71, wherein the at least one component establishes a transaction type that is to be executed for a user to gain permission to open the SSC, and when executed, the transaction type includes at

least one of a password, demographic information, device information, gathering financial data, credit card data, and personal user data.

Claim 100: The computer program product of claim 99, wherein the personal identification includes at least one of a user identification number, a company identification number, and a biometric identification.

Claim 101: The computer program product of claim 100, wherein the biometric information includes at least one of a voice data, a fingerprint data, a retina data, and a physical attribute scan data.

Claim 102: The computer program product of claim 99, wherein the device information includes gathered data from a removable storage media.

Claim 103: The computer program product of claim 99, wherein the transaction type includes a subscription transaction type that, when executed, gathers subscription data enabling a user to purchase multiple digital containers.

Claim 104: The computer program product of claim 103, wherein the subscription transaction type, that when executed, gathers subscription data enabling a user to purchase the multiple digital containers related to a pre-determined time period.

Claim 105: The computer program product of claim 71, wherein the at least one component compresses the contents of the digital container.

Claim 106: The computer program product of claim 71, wherein the at least one component incorporates a hidden key into the digital.

Claim 107: A computer program product comprising a computer usable medium having readable program code embodied in the medium, the computer program product includes at least one component to:

receive a secured streaming container (SSC) having streaming media content; and

access the SSC to acquire portions of the streaming media content while other portions of the streaming media content remain secure in the SSC.

Claim 108: The computer program product of claim 107, wherein the at least one component plays the portions of the streaming media content while other portions remain secure n the SSC.

Claim 109: The computer program product of claim 108, wherein the at least one component receives the SSC on a target device.

Claim 110: The computer program product of claim 109 wherein at least some of the contents of the SSC is configured to execute within the environment of the target device.

Claim 111: The computer program product of claim 110, wherein the target device includes at least one of a cell phone, a personal data assistant (PDA), a personal computer, a computing device, a portable music player, a tablet computer, a cable modem, a television, a cable television tuner, and a satellite receiver.

Claim 112: The computer program product of claim 107, wherein the at least one component obtains permission to access the SSC.

Claim 113: The computer program product of claim 112, wherein the permission is obtained using at least one of (i) verifying a password, (ii) demographic data, (iii) personal data, (iv) target device identification data, (v) processing a subscription transaction, and (vi) processing a financial transaction.

Claim 114: The computer program product of claim 113, wherein the personal data includes at least one of a user identification (ID), a company ID, and a biometric data.

Claim 115: The computer program product of claim 113, wherein the target device identification data includes at least one of an input from a removable storage media and an input provided from a secure device attached to the target device.

Claim 116: The computer program product of claim 107, wherein the at least one component reads extensible markup language tags (XML) to determine at least one of a content file title, a digital rights management descriptor, a file size and a file type.

Claim 117: The computer program product of claim 107, wherein the at least one component decrypts the SSC.

Claim 118: The computer program product of claim 107, wherein the at least one component decompresses the streaming media content.

Claim 119: The computer program product of claim 118, the at least one component decodes the streaming media content as a hyper-text markup language (html) file.

Claim 120: The computer program product of claim 107, wherein the at least one component downloads a java applet in order to read the contents of the SSC.

Claim 121: The computer program product of claim 107, wherein the at least one component requires a password for subsequent SSC access.

Claim 122: The computer program product of claim 107, wherein the at least one component:

successfully gains permission to the SSC on a target device;

sends a portion of data uniquely associated with the target device to a verification server;

combines the portion of data and a digital container identification data previously registered with the verification server to produce a permission token,

sends the permission token to the target device; and

rekeys an original key sent with the SSC using the permission token to securely rekey the streaming media content so that decrypting the streaming media content is locked to and performed only on the target device.

Claim 123: The computer program product of claim 108, wherein the at least one component:

detects an attempt to access the SSC;

determines if permission has been previously granted to open the SSC and, if not,

supplies transaction information;

sends the transaction information to a digital container verification server in an encrypted session and the digital container verification server sends a permission token back to the SSC; and

the at least one component grants permission to open the SSC.

Claim 124: The computer program product of claim 123, wherein the transaction information includes at least one of a financial information, a personal data, and a demographic data.

Claim 125: The computer program product of claim 124, wherein the financial information is credit card information.

Claim 126: The computer program product of claim 124, wherein the personal data is biometric data.

Claim 127: The computer program product of claim 108, wherein the at least one component plays the streaming media content from a location on a target device so that the streaming media content plays without interruption avoiding network connectivity delays and disruptions.

Claim 128: The computer program product of claim 127, wherein the at least one component requires a password to replay the streaming media content.

Claim 129: The computer program product of claim 108, wherein the streaming media content is protected and cannot be copied.

Claim 130: A method of receiving information comprising the steps of:

receiving a secured streaming container (SSC) having streaming media content;

accessing the SSC using management controls; and

playing the streaming media content on a target device wherein the streaming media content by-passes non-volatile memory or persistent storage.

Claim 131: A streaming media apparatus, comprising:

a means for controlling access to a digital container having streaming media content;

a means for securely streaming the streaming media content from the digital container once access is obtained to the digital container; and

a means for playing the streaming media content such that one or more segments of the streaming media content are sequentially presented to a media player from the digital container while remaining segments of the streaming media content remain secure in the digital container until sequentially played.

Claim 132: The streaming media apparatus of claim 131, wherein streaming media content is one or more encrypted files of streaming media content and the means for securely streaming includes a means for streaming the one or more

encrypted files of streaming media content so that the one or more files are invulnerable to copying or unauthorized access.